BUREAU DU CONSEIL PRIVÉ

Évaluation des risques associés aux fonds de renseignements personnels

Division de la vérification et de l'évaluation

Rapport final

19 août 2016

Table des matières

Acronymes utilisés dans ce rapport ii

1.0 Présentation 1

2.0 Autorisation 1

3.0 Objectifs 1

4.0 Portée 1

5.0 Contexte 1

6.0 Approche, méthodologie et critères d'évaluation 2

7.0 Un cadre de gestion des renseignements personnels fondé sur les PPRP 2

7.1 Gouvernance et responsabilisation 4

7.2 Surveillance de la conformité 4

7.3 Gestion des risques 5

7.4 Mesures de protection 6

7.5 Sensibilisation 7

8.0 Conclusion de l'évaluation des risques 8

APPENDICE A – Importance des risques cernés 10

APPENDICE B : Fichiers de renseignements personnels 13

APPENDICE C – Liste des personnes interrogées (par titre) 16

Acronymes utilisés dans ce rapport

AIPRP	Accès à l'information et protection des renseignements personnels
BCP	Bureau du Conseil privé
CSGI	Cadre supérieur responsable de la gestion de l'information
CT	Conseil du Trésor
ÉFVP	Évaluation des facteurs relatifs à la vie privée
FRP	Fichiers de renseignements personnels (FRP)
GC	Gouvernement du Canada
GI	Gestion de l'information
OPSEC	Opérations de la sécurité
PPRP	Principes généralement reconnus en matière de protection des renseignements personnels
PVRF	Plan de vérification fondé sur les risques
RH	Ressources humaines
SMA-SM	Sous-ministre adjointe (Services ministériels)

1.0 Présentation

Les Canadiens et Canadiennes attachent de l'importance à la vie privée et à la protection de leurs renseignements personnels. Ils s'attendent à ce que les institutions fédérales respectent l'esprit et les exigences de la *Loi sur la protection des renseignements personnels* (la Loi). Le gouvernement du Canada (GC) reconnait qu'il est essentiel de protéger ces renseignements pour maintenir la confiance du public dans ses institutions. C'est pourquoi il s'engage à préserver la vie privée en protégeant adéquatement tous les renseignements personnels sous son contrôle.

2.0 Autorisation

Le greffier a approuvé l'évaluation des risques associés aux fonds de renseignements personnels dans le cadre du Plan de vérification fondé sur les risques (PVFR) 2015-2016 à 2017-2018 du Bureau du Conseil privé (BCP).

3.0 Objectifs

La présente évaluation avait pour objet de :

i. cerner les risques associés à la protection et à la gestion des renseignements personnels que détient le BCP;

ii. évaluer l'importance relative des risques en fonction de la probabilité d'occurrence de chaque risque et de son impact éventuel;

iii. déterminer si les contrôles existants décrits par la direction et soumis à des tests limités lors de l'évaluation des risques pourront prévenir ou atténuer les risques les plus importants.

4.0 Portée

Cette évaluation des risques porte sur l'ensemble du Ministère. Les fonds de renseignements personnels du BCP y sont définis et consignés, notamment où ces fonds existent, et les contrôles et les processus utilisés par le BCP pour gérer ces fonds y sont examinés. Les fichiers de renseignements personnels (FRP) qui se trouvent sur Info Source font partie de l'évaluation. Dans Info Source, ou trouve de l'information sur les catégories de renseignements personnels recueillis par le BCP, ainsi que sur la façon dont ces renseignements doivent être traités, utilisés, conservés et éliminés. Étant donné qu'il ne s'agissait que d'une évaluation des risques et non d'une vérification, des contrôles limités ont été faits.

5.0 Contexte

Lors des deux derniers processus annuels de planification de la vérification, on a soulevé des questions sur le volume de renseignements personnels détenus par le BCP et sur la façon dont ces renseignements sont gérés. En réponse, ce projet d'évaluation des risques a été ajouté au PVFR approuvé par le greffier. La Loi et le Règlement connexe sur la protection des renseignements personnels sont la toile de fond de cette évaluation des risques puisqu'ils fournissent le cadre législatif lié à la création, à la collecte, à la conservation, à l'utilisation, à la divulgation, à l'assurance de l'exactitude et à l'élimination des renseignements personnels utilisés par les institutions gouvernementales pour l'administration des programmes et des activités. Les conséquences de toute lacune dans les pratiques de gestion de l'information appliquées aux fonds de renseignements personnels sur la réputation du BCP sont considérées comme importantes.

On utilisera les résultats de cette évaluation des risques pour guider les prises de décisions et le processus de planification de la vérification annuelle de l'an prochain.

6.0 Approche, méthodologie et critères d'évaluation

En 2009, l'Institut canadien des comptables agréés et l'American Institute of Certified Public Accountants, Inc. ont mis sur pied un groupe de travail sur la protection des renseignements personnels, et ce groupe a créé un cadre de protection des renseignements personnels : les *Dix principes généralement reconnus en matière de protection des renseignements personnels* (PPRP). Ces principes ont été établis à partir de différentes politiques, exigences réglementaires et pratiques exemplaires internationales, mais sont néanmoins conformes aux autorités concernant les fonds de renseignements personnels et la protection de la vie privée du GC. Ces dix principes sont les suivants : (1) gestion; (2) avis; (3) choix et consentement; (4) collecte; (5) utilisation, conservation et élimination; (6) accès; (7) divulgation à des tiers; (8) sécurité de la vie privée; (9) qualité; (10) contrôle et conformité.

Ces dix principes sont souvent utilisés à titre de référence et de critères dans les vérifications et les évaluations des risques associés aux fonds de renseignements personnels. Pour des raisons pratiques, nous les avons regroupés en cinq (5) catégories à la section 7.0 : (i) gouvernance et responsabilité; (ii) surveillance de la conformité; (iii) gestion des risques; (iv) protection; (v) sensibilisation.

La méthode adoptée dans cette évaluation des risques comprend la détermination des risques, l'analyse des risques et l'évaluation des risques. En faisant cette évaluation, l'équipe du projet :

- a mené des entrevues auprès des membres de la direction et du personnel du Ministère;
- a regroupé, examiné et analysé la documentation clé, y compris la Loi et le Règlement connexe sur la protection des renseignements personnels, et les autres autorités qui s'appliquent, notamment les politiques, les normes et les lignes directrices du Conseil du Trésor (CT);
- a fait des tests de cheminement limités des processus et des contrôles clés.

Les résultats de l'évaluation des risques ont été communiqués aux supérieurs hiérarchiques et un rapport préliminaire a été préparé et soumis à l'approbation de la sous-ministre adjointe Services ministériels (SMA-SM), étant donné qu'elle assume le rôle de cadre supérieur responsable de la gestion de l'information (CSGI) au BCP. Les rapports préliminaires du projet préparés par la Division de la vérification et de l'évaluation du BCP sont présentés au Comité de vérification du BCP pour examen et approbation, après quoi ils sont recommandés conjointement au greffier pour approbation formelle.

7.0 Un cadre de gestion des renseignements personnels fondé sur les PPRP

Le tableau ci-dessous est un cadre de gestion des renseignements personnels fondé sur le regroupement des dix PPRP en cinq (5) catégories générales, tel que décrit ci-dessus.

Gouvernance et responsabilité	Surveillance de la conformité	Gestion des risques	Protection	Sensibilisation
Gestion	Surveillance et application de la loi	Collecte Utilisation, conservation et élimination Divulgation à des tiers. Qualité	Sécurité.	Avis Accès Choix et consentement :

Le BCP a des structures et des mécanismes de contrôle interne qui s'appliquent directement ou indirectement aux questions liées à la protection des renseignements personnels et au traitement et à la protection des fonds de renseignements personnels. Comme il en est question dans la section 6.0, l'évaluation des risques a pour but d'identifier les risques liés à la protection et à la gestion des renseignements personnels sous la responsabilité du BCP (voir Appendice A).

Le tableau ci-dessous présente les résultats de cette évaluation des risques selon les cinq catégories déterminées précédemment. Il illustre comment l'équipe de l'évaluation des risques évalue la position actuelle du BCP dans chaque catégorie. La légende sous le tableau indique les trois cotes utilisées pour indiquer s'il s'agit d'une catégorie pour laquelle les préoccupations sont faibles, moyennes ou élevées.

	Évaluation des risques associés aux fonds de renseignements personnels	Cote
1	Gouvernance et responsabilité	
2	Surveillance de la conformité	
3	Gestion des risques	
4	Protection	
5	Sensibilisation	

Légende des cotes :	
	Faibles préoccupations
	Préoccupations moyennes
	Grandes préoccupations

Les sections suivantes présentent l'information descriptive sur chacune des cinq (5) catégories de PPRP. L'équipe d'évaluation utilise cette information pour évaluer chacune de ces catégories en fonction des renseignements recueillis lors de l'évaluation des risques.

7.1 Gouvernance et responsabilisation

Le BCP a une structure formelle de comités de gouvernance qui gèrent toutes les activités et les priorités du Ministère. Cette structure formelle comprend le Comité exécutif appuyé par le Comité consultatif de la gestion ministérielle, le Comité consultatif des ressources humaines et le Comité ministériel de vérification. La haute direction se réunit aussi régulièrement au Comité des opérations du BCP, où les problèmes peuvent être portés à l'attention du greffier, notamment en ce qui concerne les menaces ou les risques liés aux fonds de renseignements personnels. De nombreux comités de soutien participent également aux mécanismes et aux processus de gouvernance et de responsabilisation du BCP.

Les entrevues réalisées dans le cadre du projet ont révélé que les rôles et les responsabilités de collecte, de divulgation, d'utilisation et de conservation des renseignements personnels sont communiqués et bien compris. Le directeur de la Division de l'accès à l'information et de la protection des renseignements personnels (AIPRP) est le responsable de la protection de la vie privée pour le Ministère. Les principaux secrétariats et secteurs de programmes qui gèrent l'information personnelle sont notamment la Division des ressources humaines (RH), le Secrétariat du personnel supérieur, le Secrétariat de la jeunesse, les Opérations de la sécurité (OPSEC), et la Section de la correspondance de la haute direction. L'Unité de gestion des documents du BCP au sein de la Division des services d'information ministériels soutient les activités de gestion des fonds de renseignements personnels. L'évaluation des risques indique qu'il existe une relation de travail constructive entre ces unités opérationnelles et la Division de l'AIPRP, et que selon la *Directive du CT sur l'évaluation des facteurs relatifs à la vie privée*, les évaluations relatives à la vie privée (EFRP) sont faites par différentes unités opérationnelles et divisions de l'AIPRP avant que les nouveaux programmes soient créés. Ces activités sont dirigées par les cadres de la Division de l'AIPRP.

Conformément à la *Politique du CT de 2014 sur la protection de la confidentialité* et d'autres pouvoirs connexes, le BCP a des FRP normalisés enregistrés auprès du Secrétariat du Conseil du Trésor. Ces FRP contiennent des fonds de données personnelles sur les employés du BCP. Sous la direction du responsable de la protection de la vie privée, l'Unité des services à la clientèle de la Division de l'AIPRP met à jour annuellement ces FRP en fonction des fonds de renseignements personnels du BCP. Vous trouverez un inventaire des RFP du BCP à l'Appendice B.

7.2 Surveillance de la conformité

Le BCP doit se conformer aux autorités applicables, comme la *Loi sur la protection des renseignements personnels,* la *Politique sur la protection de la vie privée*, la *Politique sur la sécurité du gouvernement,* la *Directive sur l'évaluation des facteurs relatifs à la vie privée* et la *Directive sur les pratiques relatives à la protection de la vie privée.* Le BCP a établi des procédures, des systèmes et d'autres contrôles de collecte, de conservation, d'utilisation, de divulgation et d'élimination des renseignements personnels, et des procédures sont en place pour permettre aux employés de vérifier la conformité et d'obtenir réparation s'ils ont l'impression que leur vie privée ou leurs renseignements personnels ont été compromis.

Le cadre de gestion de l'information (GI) du BCP est bien établi. Une vérification récente faite au BCP dans le secteur de la GI a conclu que le Ministère se conformait à la grande majorité des exigences de la *Politique du CT sur la gestion de l'information* et de la *Directive sur la tenue de documents*. Pour atteindre l'objectif stratégique du gouvernement en matière d'atténuation des risques et de protection des ressources d'information stratégique, le Ministère a élaboré un ensemble d'instruments de politiques visant à définir et à appuyer les résultats et les responsabilités du BCP en matière de GI. Plus précisément, la direction a mis au point une nouvelle politique sur la gestion de l'information, qui est entrée en vigueur le 1er janvier 2014. Cette nouvelle politique définit les objectifs, les exigences stratégiques et les responsabilités du BCP en ce qui concerne la GI.

Le CSGI du BCP (SMA-DGSG) a publié la *Directive sur la tenue de documents* du BCP le 1er janvier 2014, conformément à la *Politique sur la gestion de l'information* du Ministère. Cette directive appuie les processus de gouvernance et de responsabilisation établis dans la politique et précise les processus clés de tenue des dossiers, notamment en ce qui concerne l'identification, la saisie et la conservation des renseignements ayant une valeur opérationnelle. Ces processus aident le BCP à gérer ses ressources d'information stratégique, dont les fonds de renseignements personnels, en conformité avec les exigences et les spécifications du GC.

De même, le BCP se conforme aux exigences du GC en matière de conservation et d'élimination. Les résultats de l'évaluation des risques indiquent qu'il y a un accès contrôlé à l'information, qu'elle soit sur papier ou en format électronique. Les résultats des tests de cheminement indiquent que des classeurs sécurisés avec des serrures à combinaisons sont utilisés pour conserver les renseignements personnels, conformément aux normes du GC. Le BCP utilise les procédures opérationnelles normalisées pour éliminer les ressources d'information, notamment les fonds de renseignements personnels.

Comme il a été noté ci-dessus, la Division de l'AIPRP du BCP effectue des EFVP avant la mise en œuvre des nouveaux programmes. Selon les *Lignes directrices sur l'EFVP*, un des objectifs clés d'une EFVP est de communiquer efficacement les risques pour la vie privée qui ne sont pas encadrés par d'autres mécanismes ministériels et de s'assurer que la protection de la vie privée est une considération clé dans la création initiale des objectifs et des activités d'un projet. En faisant les EFVP nécessaires, le BCP atténue les risques pour la protection de la vie privée. Cela vient renforcer la relation opérationnelle positive notée dans cette évaluation des risques entre l'AIPRP (dirigé par le responsable de la protection de la vie privée) et différentes unités opérationnelles du BCP.

7.3 Gestion des risques

Un cadre de gestion des risques est en place au BCP pour appuyer la gestion des fonds de renseignements personnels. Des mesures de contrôle et des procédures sont en place pour limiter la collecte, l'utilisation, la divulgation et la conservation des renseignements personnels. L'ensemble des mécanismes et des contrôles de gestion des risques, y compris le contrôle de l'accès aux ordinateurs et aux autres appareils électroniques, est conforme aux PPRP et permet d'atténuer les risques que des personnes non autorisées accèdent à des fonds de renseignements personnels du BCP. De plus, avec le système People Soft et d'autres outils, les employés peuvent s'assurer en permanence de l'exactitude de leurs renseignements personnels par des voies confidentielles et sûres.

Les fonds sont conservés dans des aires protégées ayant des points d'accès contrôlés bien sécurisés. Les dossiers sont conservés dans des classeurs sécurisés avec des serrures à

combinaisons et, dans le cas de la Division de l'AIPRP, un logiciel spécial d'AIPRP est utilisé pour recueillir les renseignements personnels. L'information est transmise uniquement en fonction du principe du besoin de savoir et, si cela est nécessaire, les renseignements personnels sont transmis au moyen du réseau sécurisé CABNET du BCP. Si le transfert se fait en main propre, on utilise des mallettes de sécurité verrouillées ou des enveloppes affranchies avec double emballage, conformément aux pratiques de sécurité instaurées. Dans l'ensemble, les résultats du projet de vérification indiquent que ces pratiques sont respectées à l'échelle du BCP.

Les risques sont également gérés grâce à des mesures de contrôle et de supervision des employés. Cela permet de transmettre rapidement aux échelons supérieurs les problèmes à régler. Par exemple, dans la Division de l'AIPRP, des réunions périodiques informent les employés des dossiers en cours et des problèmes actuels, une pratique qui sert également à atténuer les risques. Des évaluations du rendement sont également faites régulièrement pour que tous les problèmes de rendement soient réglés sans délai.

Au BCP, la Division des RH et OPSEC jouent également un rôle central dans la gestion des risques en s'assurant que toutes les personnes embauchées par le Ministère sont soumises aux contrôles de sécurité et que leurs antécédents sont vérifiés. Ainsi, tous les employés qui manipulent de l'information sensible et personnelle ont fait l'objet des contrôles requis avant de recevoir leurs habilitations de sécurité. Cela constitue un autre mécanisme d'atténuation des risques dans la gestion des renseignements personnels.

Bien qu'il soit difficile d'atténuer ou de prévenir les gestes volontaires d'atteinte à la vie privée, ou la divulgation intentionnelle de renseignements personnels, les accès contrôlés et les différentes couches de supervision décrites ci-dessus ont pour but de faciliter la détection et, par conséquent, l'atténuation de ce risque. Les protocoles en matière de transmission de renseignements personnels par voies électroniques (par CABNET) et de traitement des documents sont aussi des contrôles visant à réduire les risques d'atteinte à la vie privée. En outre, les mécanismes facilitant la dénonciation d'actes répréhensibles au BCP, en plus de favoriser une culture axée sur l'éthique et les valeurs, servent d'outils de dissuasion contre de tels gestes.

7.4 Mesures de protection

L'évaluation des risques a révélé que les différentes unités opérationnelles du BCP conservant des renseignements personnels ont des mesures de protection en place pour protéger ces renseignements. Même si les dépôts comme InfoXpress et People Soft comportent des risques inhérents en raison de leur nature électronique, l'introduction de mesures de protection comme le cryptage et les mots de passe sécurisés empêchent le personnel non autorisé d'accéder à l'information à diffusion restreinte. En plus des accès très limités et contrôlés, notamment grâce à des systèmes d'alarme aux dépôts où les fonds de renseignements personnels sont conservés, des classeurs adéquatement protégés avec des serrures à combinaisons, approuvés par le GC, et des dépôts de stockage protégés avec des codes sont utilisés pour conserver les données. Des tests de cheminement faits par l'équipe de l'évaluation ont indiqué que les aires et les installations de stockage étaient protégées contre les risques et les menaces environnementaux de tous les jours.

Plusieurs couches de supervision permettent de contrôler l'accès et l'utilisation des installations du BCP. Dans les unités opérationnelles du BCP, comme la Division de l'AIPRP, la Divison des RH et le Secrétariat du personnel supérieur, des ratissages de sécurité sont faits

quotidiennement pour s'assurer qu'aucun élément résiduel ne facilite les atteintes à la vie privée ou ne posent des risques pour la protection des renseignements personnels. OPSEC a également des mesures de protection et de contrôle exhaustives en place pour surveiller ses fonds de renseignements personnels. De même, des spécialistes de la gestion de l'information de l'Unité de gestion des documents (Division des services d'information ministériels) sont chargés d'aider les principales unités opérationnelles, comme la Division des RH et le Secrétariat du personnel supérieur, à gérer au quotidien leurs fonds de renseignements personnels. Ces spécialistes de la gestion de l'information sont colocalisés dans leurs secteurs opérationnels respectifs, mais relèvent du gestionnaire de l'Unité de gestion des documents.

Le cadre de gestion de l'information du Ministère constitue un autre niveau de contrôle du ministère. Le BCP, dans le cadre de sa stratégie de transformation de la tenue des dossiers 2011, a élaboré des instruments de responsabilisation en tenue des documents qui sont maintenant utilisés dans toutes les unités principales. Ces instruments fonctionnent comme des mécanismes de contrôle et de surveillance pour protéger l'intégrité des ressources d'information stratégiques du BCP. Cette stratégie de 2011 a été élaborée pour servir de feuille de route à la mise en œuvre des politiques et des normes du GC en matière de gestion de l'information stratégique. Les instruments de responsabilisation en tenue de documents exigent que les cadres des différentes unités opérationnelles, dûment désignés à cette fonction, approuvent les mesures d'intégrité et de protection des ressources d'information ayant une valeur opérationnelle dans leurs directions et leurs secrétariats respectifs. Comme il est noté plus tôt, la politique de GI du BCP désigne la SMA-DGSG comme CSGI du BCP pour superviser la protection des ressources d'information stratégiques du BCP.

Pris dans son ensemble, le Ministère possède un système de gestion de l'information ayant les mesures adéquates pour assurer la protection et l'intégrité de ses ressources d'information stratégiques, y compris les fonds de renseignements personnels.

7.5 Sensibilisation

Le BCP possède une culture de sensibilisation aux questions liées à la protection de la vie privée qui est conforme aux PPRP. Les employés semblent généralement informés de leurs droits et de leurs responsabilités concernant l'accès à leurs renseignements personnels sous le contrôle du BCP, et la modification de ceux-ci. Des procédures et des mécanismes sont en place pour favoriser l'ouverture et la transparence et pour permettre aux employés d'avoir accès à leurs renseignements personnels. Les membres du public appelés à travailler avec le BCP par l'entremise du processus de nominations par le gouverneur en conseil reçoivent les mêmes droits et possibilités d'accès.

L'Unité des services à la clientèle de la Division de l'AIPRP donne de la formation et des conseils aux employés du BCP dans le but de les sensibiliser aux questions de protection de la vie privée et aux demandes d'AIPRP. Les services de l'Unité sont affichés sur le site intranet du Ministère, et les secteurs opérationnels sont invités à demander de la formation. L'Unité offre, sur demande, de la formation individuelle et de la formation à des groupes comptant jusqu'à 20 membres. En plus de la formation offerte par l'Unité, les employés peuvent également recevoir de la formation de sources internes ou de sources extérieures au Ministère.

Le BCP possède également une forte culture fondée sur les valeurs et l'éthique, régulièrement renforcée par de l'information distribuée à tous les employés. Le message provenant des échelons supérieurs dénonce clairement tous les actes répréhensibles et les comportements contraires à l'éthique. Le Code de valeurs et d'éthique du BCP a été approuvé en avril 2012.

Les cadres, les gestionnaires et les employés du BCP en ont alors reçu des copies et ont dû confirmer formellement qu'ils l'avaient reçu. Le Code fait maintenant partie intégrante de la trousse d'information qui est remise à tous les nouveaux employés. Sous la direction du champion des valeurs et de l'éthique du niveau du secrétaire adjoint, et avec le soutien d'une équipe des RH, la promotion du Code se fait de façon active. En plus de l'information très utile sur le site intranet du BCP, des publications cycliques et des activités de publicité périodiques font la promotion du Code et des pratiques conformes à l'éthique. L'accent mis sur les valeurs et l'éthique joue un rôle essentiel pour sensibiliser les employés aux actes répréhensibles potentiels comme les gestes volontaires d'atteinte à la vie privée ou la divulgation intentionnelle de renseignements personnels.

Le site intranet du Ministère offre également des documents d'information et des publications facilement accessibles aux employés sur les façons de rapporter des soupçons d'actes répréhensibles. Ces avenues confidentielles ne sont pas seulement proposées par les RH, mais également par OPSEC et l'agent supérieur chargé de la divulgation. Un de ces instruments est le *Processus de divulgation des actes répréhensibles du BCP*. Ces documents donnent aux employés du BCP l'information nécessaire pour bien comprendre le rôle de l'agent supérieur chargé de la divulgation, la *Loi sur la protection des fonctionnaires divulgateurs d'actes répréhensibles*, et la protection donnée aux employés en vertu de la Loi.

De plus, le BCP encourage la conformité aux politiques et aux directives du GC en matière d'EFVP. Cette fonction sert également de mécanisme de sensibilisation à la protection de la vie privée et de l'intégrité des fonds de renseignements personnels du ministère. Selon les *Lignes directrices sur l'EFVP*, un des objectifs clés d'une EFVP est de communiquer efficacement les risques pour la protection de la vie privée qui ne sont pas encadrés par d'autres mécanismes ministériels. L'EFVP vise à renforcer la capacité de la haute direction de prendre des décisions éclairées en matière de politiques, de conception de système et d'approvisionnement. Conformément à leurs objectifs particuliers, ces lignes directrices favorisent la promotion de la sensibilisation aux questions liées à la vie privée et à leur compréhension, et donnent aux décideurs la capacité de prendre des décisions éclairées en matière de politiques, de conception de système et d'approvisionnement fondées sur la compréhension des risques liés à la vie privée et des options disponibles pour atténuer ces risques. Par conséquent, en faisant systématiquement des EFVP avant de mettre en œuvre de nouveaux programmes ou de créer de nouvelles entités au BCP, on favorise la culture et la sensibilisation concernant la protection des renseignements personnels et de la vie privée, et on atténue ainsi les risques associés.

Pris individuellement et collectivement, ces mécanismes de sensibilisation permettent aux employés d'accéder facilement à l'information visant à mieux les sensibiliser à la gestion des renseignements personnels. Toutefois, lorsqu'on leur demande quel domaine pourrait être généralement amélioré au BCP, la plupart des employés répondent qu'il faut continuer de chercher à améliorer la sensibilisation des employés.

8.0 Conclusion de l'évaluation des risques

Le BCP a un cadre de contrôles de gestion et d'autres mécanismes en place pour gérer les fonds de renseignements personnels. Bien que la présente évaluation des risques ait identifié des risques dans la gestion de ces fonds d'information personnels, les résultats des tests limités qui ont été faits suggèrent un haut degré de conformité aux autorités qui s'appliquent, et les mesures de contrôle en place permettront d'atténuer les risques les plus importants et de

contribuer à les prévenir. Grâce à ce cadre de contrôles, le risque résiduel d'atteinte substantielle aux fonds de renseignements personnels est considéré comme faible.

APPENDICE A – Importance des risques cernés

Cet appendice présente une liste des risques potentiels pour la gestion efficace des fonds de renseignements personnels du BCP (ci-dessous) et évalue leur importance respective selon l'Équipe de l'évaluation des risques à la fin du projet, après avoir pris en considération les mesures de contrôle en place pour atténuer la probabilité de ces risques ainsi que leur incidence sur le BCP s'ils venaient à se concrétiser.

Le tableau ci-dessous illustre la probabilité et le degré d'incidence des risques selon les cotes « faible », « moyen » et « élevé », alors que la détermination de l'importance à la conclusion du projet (selon la combinaison des facteurs de probabilités et d'incidences après la prise en considération des mesures d'atténuation) est évaluée pour chaque risque selon les cotes « négligeable », « substantielle » et « critique ».

L'incidence d'un risque peut être estimée comme moyenne ou élevée, mais le facteur le plus important est la probabilité que ce risque se concrétise.

Probabilité	Incidence	Importance
Élevé	Élevé	Critique
Moyen	Moyen	Substantielle
Faible	Faible	Négligeable

Risque	*Probabilité*	*Incidence*	*Importance*
Gouvernance et responsabilité			
1. Les rôles, les responsabilités et les obligations en matière de collecte, de divulgation, d'utilisation et de conservation des renseignements personnels ne sont peut-être pas bien définis et communiqués.	*Faible*	*Faible*	*Négligeable*
2. Les secteurs de programmes gérant les renseignements personnels ne sont peut-être pas bien définis.	*Faible*	*Faible*	*Négligeable*
3. L'atteinte aux fonds de renseignements personnels pourrait donner lieu à des préjudices ou à des atteintes à la réputation.	*Faible*	*Élevé*	*Substantielle*
4. Les processus et les contrôles applicables ne sont peut-être pas bien documentés.	*Faible*	*Faible*	*Négligeable*
5. Il n'y a peut-être pas de liste exhaustive des fonds de renseignements personnels du BCP.	*Faible*	*Faible*	*Négligeable*
Surveillance de la conformité			
1. La justification de la collecte des renseignements personnels n'est peut-être pas expliquée aux employés, minant ainsi les principes de transparence et d'ouverture.	*Faible*	*Faible*	*Négligeable*
2. Il n'y a peut-être pas de processus et de contrôles efficaces pour superviser la collecte, la conservation et l'utilisation des renseignements personnels.	*Faible*	*Moyen*	*Négligeable*
3. Les exercices de conformité, y compris les évaluations des facteurs relatifs à la vie privée, ne sont peut-être pas faits périodiquement pour vérifier le respect des lois et des règlements.	*Faible*	*Moyen*	*Négligeable*
4. Il n'y a peut-être pas de contrôles efficaces en place pour vérifier qu'on procède à la collecte, à la conservation, à l'utilisation, à la divulgation et à l'élimination des renseignements conformément aux politiques et aux directives applicables du CT.	*Faible*	*Moyen*	*Négligeable*
Gestion des risques			
1. Il n'y a peut-être pas de cadre efficace de gestion des risques au BCP pour gérer les risques associés à la collecte, à la divulgation, à l'utilisation et à la conservation des renseignements personnels.	*Faible*	*Moyen*	*Négligeable*
2. Les types de dépôts où sont stockés les renseignements personnels posent des risques inhérents qui n'ont peut-être pas été suffisamment atténués.	*Faible*	*Moyen*	*Négligeable*

3. Il n'y a peut-être pas de systèmes ou de processus adéquats en place pour déceler et corriger rapidement les atteintes à la vie privée.	*Faible*	*Moyen*	*Négligeable*
Protection			
1. Il n'y a peut-être pas de mesures de protection adéquates en place pour protéger les renseignements personnels conformément à la *Loi sur la protection des renseignements personnels*, la *Politique sur la protection de la vie privée*, la *Politique sur la sécurité du gouvernement*, la *Directive sur l'évaluation des facteurs relatifs à la vie privée* et la *Directive sur les pratiques relatives à la protection de la vie privée et d'autres exigences du GC et des PPRP.*	*Faible*	*Moyen*	*Négligeable*
2. Les fonds de renseignements personnels sont stockés dans des aires et dans des conditions qui pourraient les exposer à des risques environnementaux.	*Faible*	*Moyen*	*Négligeable*
Sensibilisation			
1. Les employés ne connaissent peut-être pas leurs droits et leurs responsabilités en matière d'accès à leurs renseignements personnels.	*Faible*	*Moyen*	*Négligeable*
2. Les employés qui ne participent pas activement à la gestion quotidienne des fonds de renseignements personnels ne connaissent peut-être pas bien l'importance accordée par le BCP à la gestion efficace de ces renseignements.	*Faible-moyen*	*Moyen*	*Négligeable-Substantielle*
3. Il n'y a peut-être pas de cadre de gestion des facteurs relatifs à la vie privée au BCP, conformément aux exigences du GC et des PPRP dans ce domaine.	*Faible*	*Moyen*	*Négligeable*
4. Les gestionnaires et les employés qui traitent les renseignements personnels ne sont peut-être pas suffisamment formés pour le faire.	*Faible*	*Moyen*	*Négligeable*
5. Il y a peut-être certaines lacunes dans la gestion des fonds de renseignements personnels du ministère qui peuvent faciliter l'atteinte intentionnelle ou non intentionnelle aux fonds de renseignements personnels conservés au Ministère.	*Faible*	*Moyen*	*Négligeable*

APPENDICE B : Fichiers de renseignements personnels

Ce sont des renseignements personnels organisés ou destinés à être récupérés au moyen du nom d'une personne ou au moyen d'un numéro d'identification, d'un symbole ou d'une autre indication attribuée uniquement à cette personne. Les renseignements personnels décrits dans le fichier de renseignements personnels ont été utilisés, sont utilisés ou sont accessibles à des fins administratives et sont sous la garde d'une institution gouvernementale.

Le SCT a élaboré des fichiers de renseignements personnels ordinaires pour décrire les renseignements personnels créés, recueillis et conservés par la plupart des institutions du gouvernement dans le cadre de leurs fonctions, activités et programmes internes courants. Vous trouverez ci-dessous les principaux fichiers de renseignements personnels :

Titre	Numéro du fichier	Numéro de renvoi au document
Demandes en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*	POU 901	NDP 930
Comptes créditeurs	POU 931	NDP 914
Comptes débiteurs	POU 932	NDP 914
Cartes d'achat	POU 940	NDP 914
Demandes d'emploi	POU 911	NDP 920
Présences et congés	POE 903	NDP 941
Planification de la continuité des activités	POU 903	NDP 928
Plaintes déposées en vertu de la *Loi canadienne sur les droits de la personne*	POU 933	NDP 926
Mesures disciplinaires	POE 911	NDP 926 et NDP 946
Divulgation d'information sur les actes fautifs commis en milieu de travail	POU 906	NDP 926 et NDP 931
Divulgation aux organismes	POU 913	NDP 937

d'enquête		
Journaux de contrôle des réseaux électroniques	POU 905	NDP 932
Aide aux employés	POE 916	NDP 922
Programme de gestion du rendement des employés	POE 912	NDP 946
Dossier personnel d'un employé	POE 901	NDP 920
Équité en emploi et diversité	POE 918	NDP 942
Correspondance à la direction	POU 902	NDP 943
Évaluation	POU 942	NDP 916
Gestion des talents des cadres supérieurs	POU 934	NDP 920
Nominations par le gouverneur en conseil	POU 918	NDP 938
Griefs	POE 910	NDP 926
Harcèlement	POE 919	NDP 922 et NDP 926
Accueil	POU 908	NDP 933 et NDP 935
Planification des ressources humaines	POU 935	NDP 949
Cartes d'identification et laissez-passer	POE 917	NDP 931
Vérification interne	POU 941	NDP 916
Communications internes	POU 915	NDP 939
Services de bibliothèque	POU 936	NDP 944
Exigences de la *Loi sur le lobbying*	POU 937	NDP 904
Membres de conseils d'administration, de comités et de conseils	POU 919	NDP 938

Santé et sécurité au travail	POE 907	NDP 922
Langues officielles	POE 906	NDP 923
Activités de sensibilisation	POU 938	NDP 904
Stationnement	POE 914	NDP 901
Rémunération et avantages	POE 904	NDP 941
Contrôle de sécurité du personnel	POU 917	NDP 920 et NDP 931
Marchés de services professionnels	POU 912	NDP 912
Communications publiques	POU 914	NDP 939
Gestion des biens immobiliers	POU 948	NDP 948
Programme de la reconnaissance	POE 920	NDP 940
Réinstallation	POU 910	NDP 936
Incidents de sécurité et atteintes à la vie privée	POU 939	NDP 931
Surveillance vidéo, registres de contrôle d'accès des visiteurs et laissez-passer	POU 907	NDP 931
Dotation	POE 902	NDP 919 et NDP 920
Formation et perfectionnement	POE 905	NDP 927
Voyages	POU 909	NDP 934 et NDP 935
Codes de valeurs et d'éthique du secteur public et Code(s) de conduite organisationnel(s)	POE 915	NDP 920 et NDP 926
Accidents d'automobile, de bateau, d'embarcation et d'avion	POE 908	NDP 922 et NDP 945

APPENDICE C – Liste des personnes interrogées (par titre)

1. Directeur exécutif, Division des ressources humaines.
2. Directeur exécutif, Opérations de la sécurité
3. Directeur et responsable de la protection de la vie privée – AIPRP
4. Directeur adjoint – AIPRP
5. Chef, Division des services à la clientèle – AIPRP
6. Analyste des politiques – AIPRP
7. Directeur, Rémunération et Développement du leadership – Division du personnel supérieur
8. Directeur, Nominations – Division du personnel supérieur
9. Gestionnaire, Gestion des documents – Division des services d'information ministériels, Services ministériels
10. Analyste principal des politiques – Secrétariat de la jeunesse
11. Conseiller en politiques – Secrétariat de la jeunesse
12. Co-dirigeant principal de l'information et directeur des opérations de TI – Direction de la gestion de l'information, des services et de la technologie